2023

Cybersecurity Terms Summary

FROM A TO Z

FREE TO USE

TABLE of contents

A **15**

Access Control List (ACL) 15
Advanced Persistent Threat (APT) 15
Adware 15
Ammy Admin 15
Antivirus 16
Authentication 16
Authorization 16
Attack Surface 16
Asset 16
Application Security 16
Advanced Encryption Standard (AES) 16
Application Programming Interface (API) 17
Access Point 17
Attack Vector 17
Air Gap 17
Authentication Factor 17
Adversary 17
Audit Trail 17
APT Framework 17
Application Whitelisting 18
Access Management 18
Authorization Token 18
Attack Tree 18
Attack Map 18
Anonymity 18
Artificial Intelligence (AI) 18
Algorithm 18
Aircrack-ng 19
Anti-spyware 19
Asset Management 19
Asymmetric Encryption 19
Application Security Testing 19
Attribute-based Access Control (ABAC) 19
Address Resolution Protocol (ARP) 19
Access Point Name (APN) 19

B **20**

Botnet 20
Brute Force Attack 20
Backup 20
Browser Hijacking 20
Bot 21

Black Hat Hacker 21
Bricking 21
Bluetooth Hacking 21
Biometric Authentication 21
Binary Code 21
Business Continuity Planning (BCP) 21
Bot Herder 22
Backdoor 22
Banner Grabbing 22
Bluejacking 22
Blacklist 22
Behavioral Analytics 22
Block Cipher 22
Blockchain Security 23
Boot Sector Virus 23
Branded Spear Phishing 23
Browser Extension Security 23
Business Email Compromise (BEC) 23
Binary Exploitation 23
Beaconing 23
Business Impact Analysis (BIA) 24
Blind SQL Injection 24
Binary Tree 24
Browser Isolation 24
Bot Imitation 24
Big Data Analytics 24
Behavioral Biometrics 24
Bootkit 25
Blind Spot 25
Botmaster 25
Browser Sandbox 25
Blockchain Mining 25
Beacon Frequency 25
Behavioral Detection 25
Bit 26
Business Process Compromise (BPC) 26
Blacklist Filter 26
Binary Analysis 26
Bitlocker 26
Bloatware 26
Bot Controller 26
Blockchain Node 27
Browser Fingerprinting 27
Biometric Authentication 27

Bypass Attack 27
Block Cipher 27
Bluejacking 27
Blackout Attack 27
Buffer Overflow 28
Bot Traffic 28
Backup and Recovery Plan 28
Baseline Security 28
Behavior-based Detection 28
Bug Bounty Program 28
BIOS Password 28
Browser Extension 29
C **30**
Cryptography 30
Cyber Attack 30
Cyberwarzone 30
Cloud Security 30
Cybersecurity Framework 31
Cyber Insurance 31
Command and Control (C2) 31
Certificate Authority (CA) 31
Content Filtering 31
Cyber Threat Intelligence (CTI) 31
Cross-Site Scripting (XSS) 31
Cyber Hygiene 31
Cybersecurity Maturity Model Certification (CMMC) 32
Credential Stuffing 32
Cyber Espionage 32
Container Security 32
Code Injection 32
Cyber Range 32
Cyber Resilience 32
Cybersecurity Information Sharing Act (CISA) 33
Cybersecurity Operations Center (CSOC) 33
Cryptocurrency Security 33
Cyber Insurance Policy 33
Cyber Kill Chain 33
Cybersecurity Risk Assessment 33
Cybersecurity Incident Response Plan (CIRP) 33
Cybersecurity Information Technology (IT) Audit 33
Cybersecurity Operations 34
Cybersecurity Frameworks and Standards 34
Cybersecurity Awareness Training 34
Cybersecurity Governance 34

Common Vulnerabilities and Exposures (CVE) 34
Cyber Deception 34
Cybersecurity Automation 34
Cybersecurity Analytics 34
Cybersecurity Culture 35
Cyber Range 35
D **36**
Data Breach 36
Dark Web 36
Data Loss Prevention (DLP) 36
Defense in Depth 37
Digital Forensics 37
Denial of Service (DoS) 37
Distributed Denial of Service (DDoS) 37
Digital Signature 37
Dumpster Diving 37
Data Classification 38
Digital Certificate 38
DNS Spoofing 38
Domain Name System (DNS) 38
Disaster Recovery 38
Data Masking 38
Digital Rights Management (DRM) 39
Data Encryption 39
Digital Identity 39
Device Management 39
Digital Watermarking 39
Deep Packet Inspection (DPI) 39
Dark Web 40
Data Leakage 40
Database Security 40
Denial of Service (DoS) 40
Digital Forensics 40
Data Loss Prevention (DLP) 40
Dual Factor Authentication (2FA) 41
Deception Technology 41
E **42**
Encryption 42
Endpoint Security 42
Exploit 42
Ethical Hacker 42
Email Spoofing 43
Endpoint Detection and Response (EDR) 43
Encryption Key 43

Encryption Algorithm 43
Eavesdropping 43
Enumeration 43
EDR Agent 43
Egress Filtering 44
F **45**
Fuzzing Attack 45
Firewall 45
Fileless Malware 45
Forensic Analysis 46
Firmware 46
Fingerprinting 46
Full Disk Encryption 46
Fraud Detection 46
File Integrity Monitoring 46
Financial Trojans 46
Federated Identity 47
Fake WAP 47
FIDO (Fast Identity Online) 47
File Transfer Protocol (FTP) 47
Fileless Persistence 47
Flaw 47
False Positive 47
Firmware Update 48
Formjacking 48
G **49**
Gray Hat Hacker 49
Gateway 49
Gone Phishing 49
Global Threat Landscape 49
Greyware 50
Ground Station 50
Gaming Malware 50
Grooming 50
GSM (Global System for Mobile Communications) 50
Ghostware 50
Geofencing 50
Google Dorking 51
GPU (Graphics Processing Unit) 51
GPG (GNU Privacy Guard) 51
Group Policy Object (GPO) 51
GEO Blocking 51
Header Manipulation 52
Honeypot 52

HTTP Response Splitting 52
Hashing 52
Hardening 53
Hardware Security Module (HSM) 53
Human error 53
HTTP (Hypertext Transfer Protocol) 53
HTTPS 53
Hybrid Cloud 53
I **54**
Incident Response Plan 54
IP Spoofing 54
Insider Threat 54
Intrusion Detection System (IDS) 55
Internet of Things (IoT) 55
IoT Security 55
Identity and Access Management (IAM) 55
Incident Response Plan 55
Incident Response Retainer 55
Injection Attack 55
J **56**
JSON Web Token (JWT) 56
JavaScript Hijacking 56
Jailbreaking 56
JavaScript Injection 56
Juice Jacking 57
Java Security 57
K **58**
Keylogger 58
Kernel 58
Kerberos 58
Kill Chain 59
Kali Linux 59
Key Exchange 59
L **60**
Lateral Movement 60
Log Analysis 60
Least Privilege 60
Logic Bomb 60
Load Balancer 61
LDAP Injection 61
Layer 2 61
Live Forensics 61
Local Area Network (LAN) 61
M **62**

Malware 62
Man-in-the-Middle Attack (MITM) 62
Mobile Device Management (MDM) 62
Metadata 62
Multi-Factor Authentication (MFA) 63
Malware Analysis 63
Machine Learning 63
Managed Detection and Response (MDR) 63
Managed Security Services (MSS) 63
Managed Vulnerability Scanning 63
Memory Forensics 64
N **65**
Network Segmentation 65
NIST (National Institute of Standards and Technology) 65
NIST Cybersecurity Framework 65
Netcat 65
Nmap 66
Network Address Translation (NAT) 66
Nonce 66
Network Tap 66
NAC (Network Access Control) 66
Network Sniffer 66
NTLM (NT LAN Manager) 66
Nessus 67
Network Protocol 67
Network Security 67
Network Architecture 67
Network Topology 67
Network Administrator 67
NAT Traversal 67
Network Forensics 68
Next-Generation Firewall (NGFW) 68
Noob 68
NTP (Network Time Protocol) 68
Null Byte Injection 68
Node.js Security 68
Near Field Communication (NFC) 68
Non-Repudiation 69
NFT (Non-Fungible Token) 69
O **70**
OAuth 70
Obfuscation 70
OSI Model (Open Systems Interconnection Model) 70
Onion Routing 70

OpenVPN 71
Operating System 71
Out-of-Band Authentication 71
OTP (One-Time Password) 71
Online Identity 71
Outdated Software 71
Onion Network 71
Offensive Security 71
Overprivileged Users 72
Obscure Web Attacks 72
Off-Path Attack 72
Over-the-Air (OTA) Updates 72
Orphaned Accounts 72
On-premises Security 72
Open Source Intelligence (OSINT) 72
Orchestration 73
P **74**
Patch 74
Payload 74
Payload Encryption 74
Penetration Testing 74
Phishing 75
Ping of Death 75
Plaintext 75
Port 75
Privilege Escalation 75
Protocol 75
Proxy Server 75
Public Key Infrastructure (PKI) 76
Password Manager 76
Physical Security 76
Packet 76
Packet Sniffing 76
Patch Management 76
Point-to-Point Tunneling Protocol (PPTP) 76
Post-Quantum Cryptography 77
Privacy Policy 77
Persistence 77
Package 77
PIP 77
Q **78**
Quantum Cryptography 78
Query Language 78
Quarantine 78

Quality of Service (QoS) 78
Quick Response (QR) Code 79
Query String 79
Queue 79
Quantum Key Distribution 79
Quorum-Based Consensus Algorithm 79
Qubes OS 79
R **80**
Radio Frequency Identification (RFID) 80
Rainbow Table 80
RADIUS (Remote Authentication Dial-In User Service) 80
Ransomware 80
Ransomware-as-a-Service (RaaS) 81
Real-Time Monitoring 81
Real-Time Threat Detection 81
Recovery Time Objective (RTO) 81
Red Team 81
Redaction 81
Redundancy 82
Reflection Attack 82
Regulated Data 82
Regulatory Compliance 82
Relay Attack 82
Reliability 82
Remote Access Trojan (RAT) 82
Remote Code Execution (RCE) 83
Remote Desktop Protocol (RDP) 83
Remote Wipe 83
Replay Attack 83
Risk Assessment 83
Risk Management 83
Risk Mitigation 83
Risk Register 84
Robocall 84
Role-Based Access Control 84
Rogue Access Point 84
Rogue Antivirus 84
Rogue Certificate 84
Rogue Code 84
Rogue Device 85
Rogue DHCP Attack 85
Rogue DHCP Server 85
Rogue Gateway 85
Rogue Program 85

Rogue Scanner 85
Rogue Software 85
Rogue Wireless Network 85
Root Certificate 86
Root Password 86
S **87**
SSL (Secure Sockets Layer) 87
Sandbox 87
SQL Injection 87
Social Engineering 87
Sniffing 88
Spoofing 88
Spear Phishing 88
Session Hijacking 88
Security Information and Event Management (SIEM) 88
Security Operations Center (SOC) 88
Security Testing 89
Script Kiddie 89
Software-Defined Network (SDN) 89
Stateful Packet Inspection (SPI) 89
Steganography 89
System Hardening 90
Security Controls 90
Security Policy 90
Security Audit 90
Security Token 90
Stuxnet 91
T **92**
TCP/IP 92
Takedown 92
Tailgating 92
TACACS+ (Terminal Access Controller Access-Control System Plus) 92
Threat Hunting 93
Threat Intelligence 93
Threat Model 93
Threat Vector 93
TLS (Transport Layer Security) 93
Tokenization 93
Tor Network 93
Traceroute 93
Trap and Trace 94
Trojan Horse 94
Trust Model 94
Trust Zone 94

Two-Factor Authentication (2FA) 94
Temporal Key Integrity Protocol (TKIP) 94
Third-Party Access 94
Tunneling 94
Transcript 95
U **96**
UDP (User Datagram Protocol) 96
Unified Threat Management (UTM) 96
URL (Uniform Resource Locator) 96
User Account Control (UAC) 96
User Activity Monitoring (UAM) 97
User Behavior Analytics (UBA) 97
User Interface (UI) 97
User-Agent 97
USB Device Security 97
Unicode Encoding 97
Unsecured Network 97
UPnP (Universal Plug and Play) 98
URL Spoofing 98
USB Rubber Ducky 98
Utility Computing 98
Unified Endpoint Management (UEM) 98
Untrusted Networks 98
Uptime 98
Update 98
V **99**
Virus 99
Vulnerability 99
Virtual Private Network (VPN) 100
Virtualization 100
Voice over Internet Protocol (VoIP) 100
Virtual Machine (VM) 100
Virus Signature 100
VLAN (Virtual Local Area Network) 101
Vulnerability Assessment 101
Virus Scanner 101
Virtual Firewall 101
Voice Biometrics 101
Vulnerability Scanning 102
VPN Concentrator 102
Virtual Desktop Infrastructure (VDI) 102
Vulnerability Exploitation 102
Virtual Patching 102
Voice Phishing (Vishing) 103

Virtual Private Cloud (VPC) 103
Virtualization Sprawl 103
W **104**
WAF (Web Application Firewall) 104
WAP (Wireless Access Point) 104
WEP (Wired Equivalent Privacy) 104
Web Security 104
Wi-Fi Protected Access (WPA) 105
Worm 105
Wi-Fi 105
Whaling 105
White Hat Hacker 105
Windows Registry 105
Wi-Fi Direct 105
Weak Password 106
Wireless Network 106
Watering Hole Attack 106
Wireless Sniffing 106
Web-Based Attack 106
Wireless Penetration Testing 106
WORM (Write Once Read Many) 106
Wiping 107
Wireless Intrusion Detection System (WIDS) 107
Wireless Intrusion Detection and Prevention System (WIDPS) 107
Wireless Intrusion Prevention System (WIPS) 107
Web Shell 107
Wildcard Mask 107
Wireless LAN (WLAN) 108
Web Server 108
Workload 108
Web Crawler 108
Wireless Key Logger 108
Wireless Bridge 108
Wireless Fidelity (Wi-Fi) 108
Web Application 109
Wi-Fi Analyzer 109
War Dialing 109
Wi-Fi Pineapple 109
WAF Bypass 109
Web Scraping 109
Web Cookies 109
Web Application Security Scanner (WASS) 110
X **111**
X.509 Certificate 111

Xen Hypervisor 111
XSRF (Cross-Site Request Forgery) 111
XML External Entity (XXE) 112
XML Injection 112
XOR Encryption 112
XSS (Cross-Site Scripting) 112
Y **113**
Yara 113
YubiKey 113
YARA-L 113
YARA Rules 113
YAML 114
Yara-Rules-Generator 114
YOLO 114
Youtube Scam 114
Your Call Is Important To Us Scam 114
Z **115**
Zigbee 115
Zero-Day 115
Zero Trust 115
Zone Transfer 115
Zoo 116
Zombie 116
Z-Wave 116

A

More: https://cyberwarzone.com/cybersecurity-terms-starting-with-a/

Access Control List (ACL)

Access Control List, or ACL, is a security feature that defines which users or groups have permission to access specific resources on a computer or network.

Advanced Persistent Threat (APT)

An Advanced Persistent Threat, or APT, is a sophisticated type of cyber attack that targets a specific organization or individual over an extended period of time, with the intention of stealing sensitive data or intellectual property.

Adware

Adware is a type of software that displays unwanted advertisements on a user's computer, often bundled with other programs or downloaded without the user's knowledge.

Ammy Admin

Ammy Admin is a remote desktop software that enables users to remotely connect to and control another computer over the internet.

Antivirus

Antivirus software is a program designed to detect, prevent, and remove malicious software, such as viruses, worms, and Trojan horses, from a computer.

Authentication

Authentication is the process of verifying the identity of a user or device, usually through a username and password, biometric information, or a security token.

Authorization

Authorization is the process of granting or denying access to a resource or system based on a user's identity, role, or other criteria.

Attack Surface

An Attack Surface is the total number of vulnerabilities and entry points that an attacker can use to exploit a system or network.

Asset

An Asset is any resource, system, or data that has value to an organization and needs to be protected.

Application Security

Application Security refers to the process of designing, testing, and implementing security measures to protect software applications from unauthorized access, modification, or destruction.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric encryption algorithm used to protect sensitive data by transforming it into a format that is unreadable without the correct decryption key.

Application Programming Interface (API)

An Application Programming Interface, or API, is a set of protocols and standards that allow different software applications to communicate with each other.

Access Point

An Access Point is a device that enables wireless devices to connect to a wired network.

Attack Vector

An Attack Vector is the path or means by which an attacker gains unauthorized access to a system or network.

Air Gap

An Air Gap is a security measure that physically separates a computer or network from the internet or any other unsecured network to prevent unauthorized access or data transfer.

Authentication Factor

Authentication Factor refers to the means by which a user proves their identity, typically through something they know (e.g., a password), something they have (e.g., a security token), or something they are (e.g., biometric information).

Adversary

Adversary refers to an individual, group, or organization that launches cyber attacks against another party or entity.

Audit Trail

Audit Trail is a record of events that allows administrators to trace and examine activities and changes on a system or network.

APT Framework

APT Framework is a structured approach used to identify, prevent, and respond to Advanced Persistent Threats.